WHAT IS CLAIMED IS:

1.   A method for resolving an addressing conflict between a first processor in a first network and a second processor in a second network, the method comprising the steps of:

detecting the addressing conflict between a first address of the first processor and a second address of the second processor;

receiving from the first processor one or more packets forming a tunnel;

removing from the one or more packets information about the tunnel;

determining that the one or more packets are associated with the detected addressing conflict based on the removed tunnel information;

determining a translated address based on the removed tunnel information; and

forwarding the one or more packets based on the translated address.

2.   The method of claim 1, wherein said step of detecting further comprises the step of:

detecting that the first address is same as the second address.

3.   The method of claim 1, wherein said step of detecting further comprises the step of:

detecting that the first address is same as the second address based on information about the first processor and the tunnel.

4.   The method of claim 1, wherein said step of removing further comprises the step of:

removing information indicating an address of the tunnel.

5.   The method of claim 1, wherein said step of removing further comprises the step of:

removing information indicating an Internet Protocol (IP) address of the tunnel.

6.   The method of claim 1, wherein said step of determining that the one or more packets are associated with the detected addressing conflict further comprises the step of:

determining, based on the removed tunnel information, that the first address in the one or more packets causes the addressing conflict.

7.   The method of claim 1, wherein said step of determining the translated address further comprises the step of:

determining the translated address based on the first address.

8.   The method of claim 1, wherein said step of determining the translated address further comprises the step of:

mapping the first address into the translated address, such that the one or more packets are forwarded on a network other than the first and second networks without the addressing conflict.

9.   The method of claim 1, wherein said step of determining the translated address further comprises the step of:

mapping the first address into the translated address, such that the one or more

packets are forwarded on the second network without the addressing conflict.

10.   The method of claim 1, wherein said step of determining the translated

address further comprises the step of:

mapping the first address into the translated address, such that the one or more

packets are forwarded on the first network without the addressing conflict.

11.   The method of claim 10, further comprising the step of:

mapping, at a gateway, the first address into the translated address.

12.   The method of claim 1, wherein said step of detecting further comprises

the step of:

detecting the addressing conflict at a gateway interfacing a network other than

the first and second networks.

13.   The method of claim 1, wherein said step of detecting further comprises

the step of:

detecting the addressing conflict at a gateway interfacing the second network.

14.   The method of claim 1, wherein said step of detecting further comprises

the step of:

detecting the addressing conflict at a gateway interfacing the first network.

15.   An apparatus comprising:

a memory including code that detects an addressing conflict between a first

address of a first processor in a first network and a second address of a second

processor in a second network, receives from the first processor one or more packets

forming a tunnel, removes from the one or more packets information about the tunnel,

determines that the one or more packets are associated with the detected addressing

conflict based on the removed tunnel information, determines a translated address

based on the removed tunnel information, and forwards the one or more packets based

on the translated address; and

at least one processor that executes the code.

16.   The apparatus of claim 15, wherein said code detects that the first

address is same as the second address.

17.   The apparatus of claim 15, wherein said code detects that the first

address is same as the second address based on information about the first processor

and the tunnel.

18.   The apparatus of claim 15, wherein said code removes information

indicating an address of the tunnel.

19.   The apparatus of claim 15, wherein said code removes information

indicating an Internet Protocol (IP) address of the tunnel.

20.   The apparatus of claim 15, wherein said code determines, based on the removed tunnel information, that the first address in the one or more packets causes the addressing conflict.

21.   The apparatus of claim 15, wherein said code determines the translated address based on the first address.

22.   The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded on a network other than the first and second networks without the addressing conflict.

23.   The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded to the second network without the addressing conflict.

24.   The apparatus of claim 15, wherein said code maps the first address into the translated address, such that the one or more packets are forwarded to the first network without the addressing conflict.

25.   The apparatus of claim 15, further comprising:

code that maps, at a gateway, the first address into the translated address.

26.   A system, comprising:

means for detecting an addressing conflict between a first address of a first processor on a first network and a second address of a second processor on a second network;

means for receiving from the first processor one or more packets forming a tunnel;

means for removing from the one or more packets information about the tunnel;

means for determining that the one or more packets are associated with the detected addressing conflict based on the removed tunnel information;

means for determining a translated address based on the removed tunnel information; and

means for forwarding the one or more packets based on the translated address.

27.   The system of claim 26, wherein said means for detecting detects that the first address is same as the second address.

28.   The system of claim 26, wherein said means for detecting detects that the first address is same as the second address based on information about the first processor and the tunnel.

29.   The system of claim 26, wherein said means for removing removes from the one or more packets information indicating an address of the tunnel.

30. The system of claim 26, wherein said means for removing removes from the one or more packets information indicating an Internet Protocol (IP) address of the tunnel.

31. A network, comprising:

a first processor having a first address on a first network;

a second processor having a second address on a second network; and

a processor other than the first and second processors that detects a conflict between the first address and the second address and resolves the conflict based on information about a tunnel established between the other processor and the first network, such that communication between the first processor and the second network is enabled.

32. The network of claim 31, wherein the other processor determines a translated address based on the information about the tunnel and forwards one or more packets to the second network based on the translated address.

33. The network of claim 31, wherein the other processor functions as a gateway.

34. The network of claim 31, wherein the other processor resolves the conflict based on information about another tunnel established between the other processor and the second network.

35.   The network of claim 31, wherein the other processor resolves the conflict

such that communication between the second processor and first network is enabled.